IN THE CLAIMS

Please amend claims 1, 5, 7, 9-11, 13, 14, 17, 19, 20, 23, 26, 30, 32, 34-37, 40, and 42 as set forth below.

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. **(Currently Amended)** A network computer system for providing security, wherein the network computer system comprises:

a monitoring function for the network computer system;

at least one outside server for an untrusted computer network, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one outside server for the untrusted computer network;

at least one proxy server, wherein the at least one outside server for the untrusted computer network is able to read and write data to the at least one proxy server, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one proxy server;

at least one inside server, wherein the at least one proxy server is able to read and write data to the at least one inside server, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one inside server; and

a core operating system that is a portion of an operating system, wherein the at least one outside server, the at least one proxy server and the at least one inside server can read and execute data from, but cannot write data to, the core operating system.

2. **(Original)** The network computer system as set forth in Claim 1, wherein the monitoring function includes at least one system level auditing function.

3. **(Original)** The network computer system as set forth in Claim 1, wherein the at least one system level auditing function resides within a first compartment and the at least one system level auditing function transports system log protocol events, generated by the operating system, through the network computer system without providing access to the system log protocol events from the at least one outside server, the at least one proxy server and the at least one inside server.

4. **(Original)** The network computer system as set forth in Claim 1, wherein the monitoring function includes at least one intrusion detection system.

5. **(Currently Amended)** The network computer system as set forth in Claim 4, wherein the at least one intrusion detection system resides within a second compartment and a third compartment, wherein the second compartment monitors activity and makes comparisons to known patterns that may indicate an attack on the network computer system and the third compartment includes source code for the intrusion detection system, wherein the second compartment can read and execute data from, but cannot write data to, ~~located in~~ the third compartment ~~without modification thereof~~.

6. **(Original)** The network computer system as set forth in Claim 1, wherein the monitoring function includes at least one system health monitoring tool.

7. **(Currently Amended)** The network computer system as set forth in Claim 6, wherein the at least one system health monitoring tool resides within a fourth compartment and a fifth compartment, wherein the fourth compartment monitors health and response time for the network computer system, and the fifth compartment includes source code for the system health monitoring tool, wherein the fourth compartment can read and execute data from, but cannot write data to, ~~located in~~ the fifth compartment ~~without modification thereof~~.

8. **(Original)** The network computer system as set forth in Claim 1, wherein the monitoring function includes at least one integrity check system.

9. **(Currently Amended)** The network computer system as set forth in Claim 8, wherein the at least one integrity check system resides within a sixth compartment and a seventh compartment, where in the sixth compartment will provide an integrity check function to monitor changes to a baseline configuration of the network computer system and the seventh compartment includes source code for the integrity detection system, wherein the sixth compartment can read and execute the source code from, but cannot write data to, ~~located in~~ the seventh compartment ~~without modification thereof~~.

10. **(Currently Amended)** The network computer system as set forth in Claim 1, wherein the monitoring function includes the at least one system level auditing function, wherein the at least one system level auditing function resides within a first compartment and the system level auditing function transports system log protocol events, generated by the operating system, through the network computer system without providing access to the system log protocol events

from the at least one outside server, the at least one proxy server and the at least one inside server and the monitoring function includes at least one intrusion detection system, wherein the at least one intrusion detection system resides within a second compartment and a third compartment, wherein the second compartment monitors activity and makes comparisons to known patterns that may indicate an attack on the network computer system and the third compartment includes source code for the at least one intrusion detection system, wherein the second compartment can read and execute data from, but cannot write data to, the third compartment ~~without modification thereof~~ and wherein at least one system health monitoring tool resides within a fourth compartment and a fifth compartment, wherein the fourth compartment monitors health and response time for the at least one outside server, the at least one proxy server and the at least one inside server and the fifth compartment includes source code for the at least one system health monitoring tool, wherein the fourth compartment can read and execute data from, but cannot write data to, the fifth compartment ~~without modification thereof~~ and wherein at least one integrity check system resides within a sixth compartment and a seventh compartment, wherein the sixth compartment will provide an integrity check function to monitor changes to a baseline configuration of the network computer system and the seventh compartment includes the source code for the integrity detection system, wherein the sixth compartment can read and execute data from, but cannot write data to, the seventh compartment ~~without modification thereof~~.

11. **(Currently Amended)** The network computer system as set forth in Claim 1, wherein the at least one outside server includes at least one eighth compartment where outside requests are received, processed, and then passed to the at least one proxy server for further processing and at least one ninth compartment where source code for the at least one outside server resides, wherein the at least one eighth compartment can read and execute data from, but

cannot write data to, the at least one ninth compartment and the at least one ninth compartment can read and execute data from, but cannot write data to, the core operating system.

12. **(Original)** The network computer system as set forth in Claim 11, wherein the source code includes encryption binaries and configuration files.

13. **(Currently Amended)** The network computer system as set forth in Claim 10, wherein the outside server includes at least one eighth compartment where outside requests are received, processed, and then passed to the at least one proxy server for further processing and at least one ninth compartment where source code for the at least one outside server resides, wherein the at least one eighth compartment can read and execute data from, but cannot write data to, the at least one ninth compartment and the at least one ninth compartment can read and execute data from, but cannot write data to, the at least one core operating system that resides in a fourteenth compartment and the third compartment of the intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one eighth compartment for the at least one outside server.

14. **(Currently Amended)** The network computer system as set forth in Claim 1, wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server, which are then passed to the at least one inside server for further processing and at least one eleventh compartment wherein source code for the at least one proxy server resides, where the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one

eleventh compartment and the at least one eleventh compartment can read and execute data from, but cannot write data to, the core operating system.

15. **(Original)** The network computer system as set forth in Claim 14, wherein the source code includes binaries and configuration files.

16. **(Original)** The network computer system as set forth in Claim 14, wherein the at least one proxy server makes buffer checks and file extension requests to ascertain whether a security threat is present.

17. **(Currently Amended)** The network computer system as set forth in Claim 10, wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server which are then passed to the at least one inside server for further processing and at least one eleventh compartment where source code for the at least one proxy server resides, wherein the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one eleventh compartment and the at least one eleventh compartment can read and execute data from, but cannot write data to, the core operating system, residing in a fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one tenth compartment for the at least one proxy server.

18. **(Original)** The network computer system as set forth in Claim 17, wherein the source code includes binaries and configuration files.

19. **(Currently Amended)** The network computer system as set forth in Claim 1, wherein the at least one inside server includes at least one twelfth compartment where the at least one inside server executes all requests received from the untrusted computer network that have been screened and deemed valid for further processing and at least one thirteenth compartment where source code for the at least one inside server resides, wherein the at least one twelfth compartment can read and execute data from, but cannot write data to, the at least one thirteenth compartment and the at least one thirteenth compartment can read and execute data from, but cannot write data to, the core operating system.

20. **(Currently Amended)** The network computer system as set forth in Claim 10, wherein the at least one inside server includes at least one twelfth compartment where the at least one inside server executes all requests received from the untrusted computer network have been screened and deemed valid for further processing and at least one thirteenth compartment where binaries and configuration files for the at least one inside server reside, wherein the at least one thirteenth compartment can read and execute data from, but cannot write data to, the core operating system, residing in a fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one twelfth compartment for the at least one inside server.

21. **(Original)** The network computer system as set forth in Claim 1, wherein system log protocol events produced by external devices can be forwarded through the at least one outside server, the at least one proxy server, and the at least one inside server to at least one other software application that monitors security intrusions.

22. **(Original)** The network computer system as set forth in Claim 1, wherein external data received from the outside through an untrusted computer network can pass from the at least one outside server wherein data from the at least one outside server can be read and written to the at least one proxy server, wherein data from the at least one proxy server can be read and written to the at least one inside server, wherein data from can at least one inside server can be read and written to at least one software application for further processing.

23. **(Currently Amended)** A network computer system for providing security, wherein the network computer system comprises:

at least one system level auditing function, wherein the at least one system level auditing function resides within a first compartment and the at least one system level auditing function transports system log protocol events produced by an operating system through the network computer system;

at least one intrusion detection system, wherein the at least one intrusion detection system resides within a second compartment and a third compartment, wherein the second compartment monitors activity and makes comparisons to known patterns that may indicate an attack on the network computer system and the third compartment is where source code for the intrusion detection system resides, wherein the second compartment can read and execute data <u>from, but cannot write data to,</u> the third compartment ~~without modification thereof~~;

at least one system health monitoring tool, wherein the at least one system health monitoring tool resides within a fourth compartment and a fifth compartment, wherein the fourth compartment monitors health and response time for the at least one outside server, the at least one proxy server and the at least one inside server and the fifth compartment is where source

code for the system health monitoring tool resides, wherein the fourth compartment can read and execute data from, but cannot write data to, the fifth compartment ~~without modification thereof~~;

at least one integrity check system, wherein the at least one integrity check system resides within a sixth compartment and a seventh compartment, wherein the sixth compartment will provide an integrity check function to monitor changes to a baseline configuration of the network computer system and the seventh compartment is where source code for the integrity check system resides, wherein the sixth compartment can read and execute the source code from, but cannot write data to, the seventh compartment ~~without modification thereof~~;

at least one core operating system, residing within a fourteenth compartment;

at least one outside server for an untrusted computer system, wherein the outside server includes at least one eighth compartment where outside requests are received and processed and at least one ninth compartment where source code for the at least one outside server resides, wherein the at least one eighth compartment can read and execute data from, but cannot write data to, the at least one ninth compartment and the at least one ninth compartment can read and execute data from, but cannot write data to, the at least one core operating system that resides in the fourteenth compartment and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one outside server;

at least one proxy server, wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server and at least one eleventh compartment where source code for the at least one

proxy server resides, wherein the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one eleventh compartment and the at least one eleventh compartment can read and execute data from, but cannot write data to, the at least one core operating system, residing in the fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one proxy server; and

wherein the at least one inside server includes at least one twelfth compartment where the at least one inside server executes all and requests received from the file unsecured computer network have been screened and deemed valid for further processing by the at least one proxy server and at least one thirteenth compartment where source code for the at least one inside server resides, wherein the at least one twelfth compartment can read and execute data from, but cannot write data to, the at least one thirteenth compartment and the at least one thirteenth compartment can read and execute data from, but cannot write data to, the at least one core operating system, residing in the fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one inside server.

24. **(Original)** The network computer system as set forth in Claim 23, wherein system log protocol events produced by external devices can be forwarded through the at least one outside server, the at least one proxy server, and the at least one inside server to at least one other software application that monitors security intrusions.

25. **(Original)** The network computer system as set forth in Claim 23, wherein data from the untrusted computer network can pass from the at least one outside server wherein data from at least one outside server can be read and written to the at least one proxy server, where data from at least one proxy server can be read and written to the at least one inside server, wherein data from can at least one inside server can be read and written to at least one software application for further processing.

26. **(Currently Amended)** A computer-implemented process for providing security to a network computer system comprising:

reading and executing data from at least one outside server for an untrusted computer network with a monitoring function while forbidding the monitoring function from writing data to the at least one outside server;

reading and executing data from at least one proxy server for an untrusted computer network with the monitoring function while forbidding the monitoring function from writing data to the at least one proxy server;

reading and executing data from at least one inside server for an untrusted computer network with the monitoring function while forbidding the monitoring function from writing data to the at least one inside server;

reading and writing data from the at least one outside server to the at least one proxy server;

reading and writing data from the at least one proxy server to the at least one inside server; and

reading and executing data from a core operating system, which is at least a portion of an operating system, with the at least one outside server, the at least one proxy server and the at least one inside server while forbidding the at least one outside server, the at least one proxy server and the at least one inside server from writing data to the core operating system.

27. **(Original)** The process for providing security to a network computer system as set forth in Claim 26, wherein the monitoring function includes auditing of the network computer system.

28. **(Original)** The process for providing security to a network computer system as set forth in Claim 27, wherein the auditing of the network computer system, within a first compartment, includes transporting system log protocol events, generated by the operating system, through the network computer system without providing access to the system log protocol events from the at least one outside server, the at least one proxy server and the at least one inside server.

29. **(Original)** The process for providing security to a network computer system as set forth in Claim 26, where in the monitoring function includes detecting of intrusions in the network computer system.

30. **(Currently Amended)** The process for providing security to a network computer system as set forth in Claim 29, wherein the detecting of intrusions includes monitoring activity and making comparisons to known patterns that may indicate an attack on the network computer system within at least one second compartment and providing source code for the monitoring activity and making comparisons to known patterns that may indicate an attack on the network computer system within at least one third compartment and reading and executing data located in

the at least one third compartment from the at least one second compartment while forbidding the at least one second compartment from writing data to the at least one third compartment.

31. **(Original)** The process for providing security to a network computer system as set forth in Claim 26, wherein the monitoring function includes monitoring health of the network computer system.

32. **(Currently Amended)** The process for providing security to a network computer system as set forth in Claim 31, wherein the monitoring health of the network computer system includes monitoring health and response time for the network computer system, within at least one fourth compartment, and providing source code for monitoring health and response time for the network computer system, within at least one fifth compartment, wherein the at least one fourth compartment can read and execute data from, but cannot write data to, ~~located in~~ the at least one fifth compartment.

33. **(Original)** The process for providing security to a network computer system as set forth in Claim 26, wherein the monitoring function includes checking of integrity of the network computer system.

34. **(Currently Amended)** The process for providing security to a network computer system as set forth in Claim 33, wherein the checking of integrity' of the network computer system includes monitoring changes to a baseline configuration of the network computer system, within the at least one sixth compartment, and providing source code for monitoring changes to a baseline configuration of the network computer system, within the at least one seventh compartment, where in the at least one sixth compartment can read and execute data from, but cannot write data to, ~~located in~~ the at least one seventh compartment.

35. **(Currently Amended)** The process for providing security to a network computer system as set forth in Claim 26, wherein the receiving of outside requests from the at least one outside server for an untrusted computer network is with the at least one eighth compartment and providing source code for receiving of outside requests from the at least one outside server for the untrusted computer network is with the at least one ninth compartment, wherein the at least one eighth compartment can read and execute data from, but cannot write data to, ~~located in~~ the at least one ninth compartment.

36. **(Currently Amended)** The process for providing security to a network computer system as set forth in Claim 26, wherein ~~the reading and writing of data to the at least one proxy server is where~~ the at least one proxy server executes and filters requests from the at least one outside server with ~~the~~ at least one tenth compartment and ~~the~~ source code for executing and filtering ~~the reading and writing of data to the at least one proxy server is where the at least one proxy server executes and filters~~ requests from the at least one outside server is provided within ~~with the~~ at least one eleventh compartment, wherein the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one eleventh compartment.

37. **(Currently Amended)** The process for providing security to a network computer system as set forth in Claim 26, wherein the reading and writing of data to the at least one inside server from the at least one proxy server is with ~~the~~ at least one twelfth compartment where the at least one inside server executes all requests received from the untrusted computer network that have been screened and deemed valid for further processing and ~~the at least one thirteenth compartment where~~ source code for the at least one inside server resides within at least one thirteenth compartment, wherein the at least one twelfth compartment can read and execute data from, but cannot write data to, the at least one thirteenth compartment.

38. **(Original)** The process for providing security to a network computer system as set forth in Claim 26, further comprising forwarding system log protocol events produced by external devices through the at least one outside server, the at least one proxy server, and the at least one inside server to the at least one other software application that monitors security intrusions.

39. **(Original)** The process for providing security to a network computer system as set forth in Claim 26, further comprising:

passing data from the outside through an untrusted computer network to the at least one outside server;

reading and writing data from the at least one outside server to the at least one proxy server;

reading and writing data from the at least one proxy server to the at least one inside server; and

reading and writing data from the at least one inside server to at least one software application for further processing.

40. **(Currently Amended)** A computer-implemented process for providing security for a network computer system comprising:

utilizing a system level auditing function, wherein the system level auditing function resides within a first compartment;

transporting system log protocol events produced by an operating system through the network computer system with the system level auditing function;

utilizing an intrusion detection system, wherein the intrusion detection system resides within a second compartment and a third compartment, wherein the third compartment includes source code for the intrusion detection system;

inspecting network activity and making comparisons to known patterns that may indicate an attack on the network computer system with the second compartment of the intrusion detection system;

reading and executing data located in the third compartment with the second compartment of the intrusion detection system while forbidding the second compartment from writing data to the third compartment;

utilizing a system health monitoring tool, wherein the system health monitoring tool resides within a fourth compartment and a fifth compartment, wherein the fifth compartment includes source code for the system health monitoring tool;

monitoring health and response time for the network computer system with the fourth compartment of the system health monitoring tool;

reading and executing data located in the fifth compartment with the fourth compartment of the system health monitoring tool while forbidding the fourth compartment from writing data to the fifth compartment;

utilizing an integrity check system, wherein the integrity check system resides within a sixth compartment and a seventh compartment;

monitoring changes to a baseline configuration of the network computer system with the sixth compartment;

reading and executing source code located in the seventh compartment with the sixth compartment while forbidding the sixth compartment from writing data to the seventh compartment;

providing a core operating system residing within a fourteenth compartment;

receiving a processing outside requests with at least one outside server for an untrusted computer network, wherein the at least one outside server includes at least one eighth compartment where outside requests are received and processed and at least one ninth compartment includes source code for the at least one outside server;

reading and executing data from the at least one ninth compartment with at least one eighth compartment while forbidding the at least one eighth compartment from writing data to the at least one ninth compartment;

reading and executing data from the fourteenth compartment with at least one ninth compartment while forbidding the at least one ninth compartment from writing data to the fourteenth compartment;

reading and executing data from the at least one eighth compartment for the at least one outside server with the third compartment of the intrusion detection system, the fifth

compartment of the system health monitoring tool and the seventh compartment of the check system while forbidding the third compartment, the fifth compartment, and the seventh compartment from writing data to the at least one eighth compartment;

executing and filtering requests from the at least one outside server to the at least one proxy server, wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server and at least one eleventh compartment includes source code for the at least one proxy server;

reading and executing data from the fourteenth compartment with at least one eleventh compartment while forbidding the at least one eleventh compartment from writing data to the fourteenth compartment;

reading and executing data from the at least one tenth compartment for the at least one proxy server with the third compartment of the intrusion detection system, the fifth compartment of the system health monitoring tool and the seventh compartment of the check system while forbidding the third compartment, the fifth compartment, and the seventh compartment from writing data to the at least one tenth compartment;

executing requests received from the untrusted computer network have been screened and deemed valid for further processing by the at least one proxy server with at least one twelfth compartment for the at least one inside server and at least one thirteenth compartment includes source code for the at least one inside server;

reading and executing data from the fourteenth compartment with the at least one thirteenth compartment while forbidding the at least one thirteenth compartment from writing data to the fourteenth compartment; and

reading and executing data from the at least one twelfth compartment for the at least one inside server with the third compartment of the intrusion detection system, fifth compartment of the system health monitoring tool and the seventh compartment of the check system while forbidding the third compartment, the fifth compartment, and the seventh compartment from writing data to the at least one twelfth compartment.

41. **(Original)** The network computer system as set forth in Claim 40, further comprising forwarding system log protocol events produced by external devices through the at least one outside server, the at least one proxy server, and the at least one inside server to the at least one other software application that monitors security intrusions.

42. **(Currently Amended)** The network computer system as set forth in Claim 40, further comprising reading and writing data from the at least one inside server ~~can be read and write~~ to at least one software application for further processing.